Journal of Algebra 321 (2009) 2353–2364

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Approximation for Frobenius algebraic equations in Witt vectors

Luc Bélair [1]

Université du Québec – UQAM, Dép. de mathématiques, Case postale 8888, succursale Centre-ville, Montréal, Québec, H3C 3P8, Canada

ARTICLE INFO

Article history:
Received 10 April 2006
Available online 14 February 2009
Communicated by Laurent Moret-Bailly

Keywords:
Witt vectors
Difference ring
Discrete valuation ring
Approximation
Ultraproduct

ABSTRACT

We prove an approximation property for solutions to difference equations in excellent discrete valuation rings satisfying an appropriate Hensel's lemma, analog to a theorem of Greenberg [M. Greenberg, Rational points in henselian discrete valuation rings, Publ. Math. Inst. Hautes Études Sci. 31 (1966) 59–64]. In the case of Witt vectors we obtain a Nullstellensatz for Frobenius algebraic equations.

1. Introduction

In [12], Greenberg proves an approximation property for solutions to polynomial systems of equations in excellent henselian discrete valuation rings. This was generalized by M. Artin, and subsequently gave rise to a theory of *Artin approximation*, culminating in Popescu's proof of Artin's conjecture that any excellent henselian local ring has this approximation property. For all this, we refer to [21]. Consider polynomial equations where an automorphism and its iterates would occur, so-called *difference equations*. In this paper, we prove a result analog to Greenberg's (Theorem 3.1) for difference equations in excellent discrete valuation rings satisfying an appropriate Hensel's lemma, a particular case of which is the ring of Witt vectors over an algebraically closed field with its Frobenius. A particular case was known [6] (see [25, §.7], for similar stronger approximation properties). We use the methods of [1] based on the ultraproduct construction from model theory, a natural tool in these questions (see [21]). The general case in characteristic p (in Theorem 3.1) was pointed out to us by the referee, whom we thank also for his (or her) remarks which improved this paper. We

E-mail address: belair.luc@uqam.ca.

[1] Partially supported by NSERC.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.01.021

will indicate how the results also hold for equations in differential[2] valuation rings (Theorem 4.3). Finally, in the case of Witt vectors, we apply our result to get a Nullstellensatz for Frobenius difference equations (Theorem 5.5), in the style of [19].

1.1. Notation and terminology

In this paper, all rings are commutative with 1. We use boldface for vector notation, e.g. $\mathbf{x} = (x_1, \ldots, x_n)$. For a local ring A, we will denote by $\max(A)$ its maximal ideal and by k_A its residue field. For a domain A, $Frac(A)$ will denote its field of fractions. If f is a polynomial over a ring A and φ some homomorphism with domain A, then f^φ denotes the polynomial obtained from f by making φ operate on the coefficients. We recall that a field extension L/K is said to be separable if either the characteristic is 0, or the characteristic is $p > 0$ and $L, K^{1/p}$ are linearly disjoint over K (e.g. see [16]).

A difference ring is a ring equipped with a fixed automorphism. In this context we usually denote the automorphism by σ and denote such a structure by (A, σ), where A is the underlying ring. For such (A, σ), $A[\boldsymbol{X}]_\sigma$ will stand for the ring of difference polynomials over A in the variables $X_1, \ldots, X_n$, namely the ring of standard polynomials over A in the variables $\sigma^j(X_i)$, $j \in \mathbb{N}$, $1 \leqslant i \leqslant n$.[3] The order of a difference polynomial f is the largest j such that some $\sigma^j(X_i)$ appears in f. Let $A \subseteq B$ be an extension of difference rings, and $\boldsymbol{a}$ a tuple from B. We let $A[\boldsymbol{a}]_\sigma = A[\sigma^j(\boldsymbol{a})\colon\ j \in \mathbb{Z}]$, the difference ring generated by $\boldsymbol{a}$ over A. Let $K \subseteq L$ be an extension of difference fields, and $\boldsymbol{a}$ a tuple from L. We let $K(\boldsymbol{a})_\sigma = K(\sigma^j(\boldsymbol{a})\colon\ j \in \mathbb{Z})$, the difference field generated by $\boldsymbol{a}$ over K. An element $a \in L$ is said to be *transformally transcendental over K* if the elements $\sigma^j(a)$, $j \in \mathbb{Z}$ (or equivalently $j \in \mathbb{N}$), are algebraically independent over K, and *transformally algebraic over K* otherwise. There is a natural notion of *transformal independence* and *transformal transcendence basis*. A difference ring is called periodic if it satisfies an identity of the form $\sigma^n(x) = x$ for some integer $n > 0$, and called aperiodic otherwise. Our difference rings are the inversive ones of [8]. For difference algebra we refer to [8].

A differential ring is a ring equipped with a derivation, i.e. an additive map, usually denoted by D, such that $D(xy) = xDy + yDx$. We usually denote such a structure by (A, D), where A is the underlying ring. For such (A, D), $A\{\boldsymbol{X}\}$ will stand for the ring of differential polynomials over A in the variables $X_1, \ldots, X_n$, i.e. the ring of standard polynomials over A in the variables $D^j X_i$, $j \in \mathbb{N}$, $1 \leqslant i \leqslant n$. Let $A \subseteq B$ be an extension of differential rings, and $\boldsymbol{a}$ a tuple from B. We let $A\{\boldsymbol{a}\} = A[D^j(\boldsymbol{a})\colon\ j \in \mathbb{N}]$, the differential ring generated by $\boldsymbol{a}$ over A. Let $K \subseteq L$ be an extension of differential fields, and $\boldsymbol{a}$ a tuple from L. We let $K\langle\boldsymbol{a}\rangle = K(D^j(\boldsymbol{a})\colon\ j \in \mathbb{N})$, the differential field generated by $\boldsymbol{a}$ over K. An element $a \in L$ is said to be *differentially transcendental over K* if the elements $D^j a$, $j \in \mathbb{N}$, are algebraically independent over K, and *differentially algebraic over K* otherwise. If a is differentially algebraic over K and there is some polynomial $F(X_0, \ldots, X_n)$ over A such that $F(a, Da, \ldots, D^n a) = 0$ and $\frac{\partial F}{\partial X_i}(a, Da, \ldots, D^n a) \neq 0$ for some i, then a is said to be *differentially separable over K*. There is a natural notion of *differential algebraic dependence*. In characteristic $p > 0$, because of the identity $Dx^p = 0$, the notion of "differential transcendence basis" is more subtle, and we refer to [18, Chapter II, §.9–§.10]. For differential algebra we refer to [18].

If U is a non-principal ultrafilter on $\mathbb{N}$, we will denote by $(\ )^*$ the functor *ultrapower modulo U*, which associates to each set S the set of sequences $(x_n)_{n\in\mathbb{N}}$, $x_n \in S$, modulo the equivalence relation of being equal on a set of indices belonging to U. There is a natural embedding $S \hookrightarrow S^*$ via the constant sequences. We refer to [1] for ultraproducts, in particular for properties preserved by the functor $(\ )^*$, e.g. being a henselian valuation ring.

[2] The referee pointed out that Guzy [14] obtained independently a weak version of Theorem 4.3 where the residue field is differentially closed of characteristic 0.

[3] N.B. The automorphism σ extends to $A[\boldsymbol{X}]_\sigma$, in the way suggested by the names of the variables, but is not onto. Sometimes the variables $\sigma^j(X_i)$ are taken over $j \in \mathbb{Z}$, but we will not do this here.

2. Difference discrete valuation rings

Let (A,σ) be a difference ring which is a local ring. Note that σ sends the maximal ideal of non-invertible elements onto itself and induces an automorphism of the residue field, which we will denote by $\bar{\sigma}$. Note also that, if A is a discrete valuation ring then σ has the remarkable property that x and $\sigma(x)$ always divide each other, so that the associated valuation on $Frac(A)$ is an *isometry*, i.e. $\sigma(x)$ has same valuation as x.

A natural example is given by a power series ring $k[[T]]$ over a field k and the automorphism $\sigma_f(\sum a_n T^n) = \sum f(a_n)T^n$, where f is a fixed automorphism of k. The example of special interest to us will be the ring $W[\widetilde{\mathbb{F}}_p]$ of Witt vectors over the algebraic closure $\widetilde{\mathbb{F}}_p$ of the prime field of characteristic $p>0$, with its Frobenius automorphism. Namely, let $\rho:\widetilde{\mathbb{F}}_p \to W[\widetilde{\mathbb{F}}_p]$ be the multiplicative section of the residue map. Any $x\in W[\widetilde{\mathbb{F}}_p]$ has a unique expansion $x=\sum_{i=0}^{\infty}\rho(a_i)p^i$ and we have the automorphism $\sigma_p(x)=\sum_{i=0}^{\infty}\rho(a_i)^p p^i$, the *Witt Frobenius* (see e.g. [28]).

The following definition[4] is due to Scanlon [24].

Definition 2.1. Let (A,σ) be a difference ring which is a valuation ring. We say (A,σ) is *σ-henselian*, if for all $f\in A[X]_\sigma$, given by $f(X_0,X_1,\dots,X_n)\in A[X_0,\dots,X_n]$, i.e. $f(X)=f(X,\sigma(X),\dots,\sigma^n(X))$, and for all $y\in A$ such that $f(y)$ is a non-unit but $\frac{\partial f}{\partial X_i}(y,\sigma(y),\dots,\sigma^n(y))$ is a unit for at least one i, then there exists $x\in A$ such that $f(x)=0$ and $x-y\in f(y)A$.

The ring of Witt vectors $(W[\widetilde{\mathbb{F}}_p],\sigma_p)$ is σ-henselian (see [2,26,5]). A difference field (k,σ) is *linearly difference closed* [26] if for each $n\in\mathbb{N}$, $n>0$, and $a_0,\dots,a_n$, $b\in k$ such that $a_0a_n\neq 0$, there is $x\in k$ such that $a_0x+a_1\sigma(x)+\cdots+a_n\sigma^n(x)=b$. Any difference ring which is a complete discrete valuation ring whose residue field is linearly difference closed is σ-henselian, viz. the Witt vectors above or the power series ring above with a suitable base field k and f. We will sketch a proof of this in order to illustrate the kind of Newton approximation needed in this context. It suffices to prove the following refinement lemma.

Lemma 2.2. *Let (A,σ) be a difference ring which is a discrete valuation ring and whose residue field $(k_A,\bar{\sigma})$ is linearly difference closed. Let π be a uniformizing parameter. Suppose $y\in A$ and $f\in A[X]_\sigma$, given by $f(X_0,X_1,\dots,X_n)\in A[X_0,\dots,X_n]$, i.e. $f(X)=f(X,\sigma(X),\dots,\sigma^n(X))$, are such that $f(y)$ is a non-unit but $\frac{\partial f}{\partial X_i}(y,\sigma(y),\dots,\sigma^n(y))$ is a unit for at least one i. Then there exists $z\in A$ such that $(y-z)f(y)^{-1}$ is a unit of A, $f(z)\in f(y)\pi A$, and $\frac{\partial f}{\partial X_i}(z,\sigma(z),\dots,\sigma^n(z))$ is a unit for at least one i.*

Proof. First recall that for all $x\in A$, there is some unit $u\in A$ s.t. $\sigma(x)=xu$. Also, $f(y)\in\pi A$. We try $z=y+\epsilon$, where ϵ is to be determined. We have

$$\begin{aligned} f(z) &= f\big(y+\epsilon,\sigma(y+\epsilon),\dots,\sigma^n(y+\epsilon)\big)\\ &= f\big(y+\epsilon,\sigma(y)+\sigma(\epsilon),\dots,\sigma^n(y)+\sigma^n(\epsilon)\big)\\ &= f(y)+\sum_{i=0}^{n}\frac{\partial f}{\partial X_i}\big(y,\sigma(y),\dots,\sigma^n(y)\big)\cdot\sigma^i(\epsilon)+R(y,\epsilon)\end{aligned}$$

where the remainder $R(y,\epsilon)$ is such that $R(y,\epsilon)\in\epsilon^2A$, for all $\epsilon\in A$. Put $\epsilon=uf(y)$, with $u\in A$ a unit to be determined. We get

$$f(z)=f(y)+\sum_{i=0}^{n}\frac{\partial f}{\partial X_i}\big(y,\sigma(y),\dots,\sigma^n(y)\big)\cdot\sigma^i\big(f(y)\big)\cdot\sigma^i(u)+R(y,\epsilon).$$

[4] Similar schemes were considered in [10] for difference operators.

Fix i_0 such that $\frac{\partial f}{\partial X_{i_0}}(y, \sigma(y), \ldots, \sigma^n(y))$ is a unit and let

$$c_i = \frac{\partial f}{\partial X_i}\big(y, \sigma(y), \ldots, \sigma^n(y)\big) \cdot \sigma^i\big(f(y)\big)/f(y)$$

then $1 + \sum_{i=0}^{n} c_i \sigma^i(x)$ is a non-trivial *linear* σ-polynomial over A, with c_{i_0} a unit. Since $(k_A, \bar{\sigma})$ is linearly difference closed, let u be a solution of

$$1 + \sum_{i=0}^{n} c_i \sigma^i(u) \equiv 0 \mod \pi A.$$

Necessarily u is a unit. So we now have

$$\left(f(y) + \sum_{i=0}^{n} \frac{\partial f}{\partial X_i}\big(y, \sigma(y), \ldots, \sigma^n(y)\big) \cdot \sigma^i\big(f(y)\big) \cdot \sigma^i(u) \right) \in f(y)\pi A,$$

$$R(y, \epsilon) \in \epsilon^2 A = f(y)^2 A \subseteq f(y)\pi A.$$

Whence $f(z) \in f(y)\pi A$, and $(y - z) f(y)^{-1} = -u$ is a unit. Finally,

$$\frac{\partial f}{\partial X_{i_0}}\big(z, \sigma(z), \ldots, \sigma^n(z)\big) = \frac{\partial f}{\partial X_{i_0}}\big(y, \sigma(y), \ldots, \sigma^n(y)\big) + R_1(y, \epsilon)$$

where $R_1(y, \epsilon) \in \epsilon A \subseteq \pi A$, so that $\frac{\partial f}{\partial X_{i_0}}(z, \sigma(z), \ldots, \sigma^n(z))$ is a unit. □

3. Approximation

Recall that a discrete valuation ring A is said to be *excellent* if the fraction field of the completion of A is separable over the fraction field of A. A difference ring will be said to be excellent if its underlying ring is excellent.

We now get our main results.

Theorem 3.1. *Let (A, σ) be a difference ring which is a σ-henselian excellent discrete valuation ring. Let t be a uniformizing parameter of A, let $f_1, \ldots, f_m \in A[\boldsymbol{X}]_\sigma$ and $\boldsymbol{f} = (f_1, \ldots, f_m)$. Then there exists an integer $N \in \mathbb{N}$, depending on $\boldsymbol{f}$, such that for all $\alpha \in \mathbb{N}$, $\alpha > 0$, and for all $\boldsymbol{x} \in A$ such that $\boldsymbol{f}(\boldsymbol{x}) \equiv 0 \bmod t^{\alpha N}$, there exists $\boldsymbol{y} \in A$ such that $\boldsymbol{f}(\boldsymbol{y}) = 0$ and $\boldsymbol{y} \equiv \boldsymbol{x} \bmod t^{\alpha}$.*

Corollary 3.2. *If, for all integer $N \geqslant 1$, there exists $\boldsymbol{x} \in A$ s.t. $f_i(\boldsymbol{x}) \equiv 0 \bmod t^N$, $i = 1, \ldots, m$, then there exists $\boldsymbol{y} \in A$ s.t. $f_i(\boldsymbol{y}) = 0$, $i = 1, \ldots, m$.*

For the proof in positive characteristic, we need an improvement on the *primitive element theorem* of [8, Chapter 7, §.6, Theorem III] for completely aperiodic difference fields, namely that it holds for any *separable* extension. We recall that a difference field is called completely aperiodic if it is of characteristic 0 and aperiodic, or if it is of positive characteristic and satisfies no identity of the form $\sigma^i(x)^q = \sigma^j(x)^r$, where i, j are non-negative integers and q, r powers of the characteristic, unless $i = j$ and $q = r$. The completely aperiodic difference fields are those which do not satisfy difference polynomial identities.

Lemma 3.3. *(See [8, Chapter 5, §.5, Lemma II].) Let $K \subseteq L$ be an extension of difference fields and suppose that K is completely aperiodic. Let $f \in L[\boldsymbol{X}]_\sigma$ be a non-zero difference polynomial, then there exists $\boldsymbol{a} \in K$ such that $f(\boldsymbol{a}) \neq 0$.*

Theorem 3.4.[5] *(Cf. [8, Chapter 7, §.6, Theorem III].) Let $K \subseteq L$ be an extension of difference fields which is finitely generated and transformally algebraic. Suppose that K is completely aperiodic and the extension is separable. Then there exists $z \in L$ such that $L = K(z)_\sigma$.*

Proof. In characteristic 0 it is the theorem quoted from Cohn's book, so assume the characteristic is $p > 0$. We can assume that $L = K(\alpha, \beta)_\sigma$ for some $\alpha, \beta \in L$ which are transformally algebraic over K. Let λ be transformally transcendental over $K(\alpha, \beta)_\sigma$, and $\eta = \alpha + \lambda\beta$. Then η is transformally algebraic over $K(\lambda)_\sigma$, and we choose a non-negative integer r smallest such that for some $s \geqslant r$, $\sigma^r(\eta)$ is algebraic over $K(\lambda, \sigma(\lambda), \ldots, \sigma^s(\lambda), \eta, \ldots, \sigma^{r-1}(\eta))$. Choose an irreducible polynomial $P(X_0, \ldots, X_s, Y_0, \ldots, Y_r)$ over K such that $P(\lambda, \ldots, \sigma^s(\lambda), \eta, \ldots, \ldots, \sigma^r(\eta)) = 0$. Since $K(\alpha, \beta)_\sigma$ is a separable extension of K and $\lambda^{1/p}$ is also transformally transcendental over $K(\alpha, \beta)_\sigma$, then $K(\alpha, \beta)_\sigma$ is certainly linearly disjoint from $K^{1/p}(\lambda^{1/p})_\sigma = (K(\lambda)_\sigma)^{1/p}$ over K. It follows that $K(\lambda, \alpha, \beta)_\sigma$ is linearly disjoint from $(K(\lambda)_\sigma)^{1/p}$ over $K(\lambda)_\sigma$, and that $K(\lambda, \eta)_\sigma$ is a separable extension of $K(\lambda)_\sigma$. By the minimality of r, the transcendence degree of $K(\lambda, \ldots, \sigma^r(\eta))$ over $K(\lambda, \ldots, \sigma^s(\lambda))$ is r [8, Chapter 5, §.14, Theorem X], and we can select from $\eta, \sigma(\eta), \ldots, \sigma^r(\eta)$ a separating transcendence basis. Then for some j, $\sigma^j(\eta)$ is separable algebraic with minimal irreducible polynomial $P(\lambda, \ldots, \sigma^s(\lambda), \eta, \ldots, \sigma^{j-1}(\eta), X, \sigma^{j+1}(\eta), \ldots, \sigma^r(\eta))$. So for some j we have

$$\frac{\partial P}{\partial Y_j}\big(\lambda, \ldots, \sigma^r(\eta)\big) \neq 0.$$

Then, as in Cohn,[6] consider $H(\lambda)$ the difference polynomial in λ over $K(\alpha, \beta)_\sigma$ obtained by replacing η by $\alpha + \lambda\beta$ in $P(\lambda, \ldots, \sigma^r(\eta))$ and expanding formally. Say $H(\lambda)$ is given by $H(Z_0, \ldots, Z_s) \in K(\alpha, \beta)_\sigma[Z_0, \ldots, Z_s]$, i.e. $H(\lambda) = H(\lambda, \sigma(\lambda), \ldots, \sigma^s(\lambda))$. Because λ is transformally transcendental over $K(\alpha, \beta)_\sigma$, $H(\lambda)$ is the zero polynomial, and hence so is $\frac{\partial H}{\partial Z_j}(\lambda, \sigma(\lambda), \ldots, \sigma^s(\lambda))$ as a difference polynomial in λ. It follows that

$$\frac{\partial P}{\partial X_j}\big(\lambda, \ldots, \sigma^s(\eta)\big) + \sigma^j(\beta)\frac{\partial P}{\partial Y_j}\big(\lambda, \ldots, \sigma^s(\eta)\big) = 0.$$

Hence, $\sigma^j(\beta) \in K(\lambda, \eta)_\sigma$, whence $\beta, \alpha \in K(\lambda, \eta)_\sigma$. Let $\alpha = f/h$, $\beta = g/h$, where f, g, h are difference polynomials in λ, η with coefficients in K, and $h \neq 0$. Consider f, g, h as difference polynomials in λ with coefficients in $K(\alpha, \beta)_\sigma$, say $f = f(\lambda)$, $g = g(\lambda)$, $h = h(\lambda)$ for $f(X), g(X), h(X) \in K(\alpha, \beta)_\sigma[X]_\sigma$. By Lemma 3.3, there is $a \in K$ such that $h(a) \neq 0$. Let $z = \alpha + a\beta$. Let $f_a, g_a, h_a \in K(z)_\sigma$ be obtained from f, g, h by replacing λ by a and η by z. Then $f_a = f(a)$, $g_a = g(a)$ and $h_a = h(a) \neq 0$. It suffices now to see that $h_a\alpha = f_a$, $h_a\beta = g_a$. But this follows by going back to the relations $h\alpha = f$, $h\beta = g$ which yield the formal relations $h(X)\alpha = f(X)$, $h(X)\beta = g(X)$ in $K(\alpha, \beta)_\sigma[X]_\sigma$, and setting $X = a$. □

We now proceed to the proof of Theorem 3.1. Let v be the valuation associated to A, whose value group is $\mathbb{Z}$, and let $k = A/(t)$ be its residue field. Let U be a non-principal ultrafilter on $\mathbb{N}$ and $(\,)^*$ the corresponding ultrapower functor. Then A^* is a σ-henselian valuation ring whose associated valuation v^* has value group $\mathbb{Z}^*$ and residue field $k^* = A^*/(t)$. We will stick to σ to denote σ^*. Even though A^* is no longer a discrete valuation ring, it is still true that for all $x \in A$, $v^*(\sigma(x)) = v^*(x)$. Let H be a convex subgroup of $\mathbb{Z}^*$ containing $\mathbb{Z}$, and let $I_H = \{x \in A^*\colon\ v^*(x) \notin H\}$. Since H is convex, I_H is a prime ideal of A^*, and also $\sigma(I_H) = I_H$. Let $A^H = A^*/I_H$ and $A^* \xrightarrow{\pi} A^H$, $A \xrightarrow{i} A^*$ be the natural maps. Then A^H is a valuation ring with value group H and residue field k^*. Let σ^H be the automorphism of A^H induced by σ via π. Then i induces an embedding of A into A^H and we consider A as a difference subring of A^H.

[5] In positive characteristic, this is due to the referee. In the non-inversive context, the same argument yields the conclusion as in Cohn, i.e. there is $z \in L$ and a non-negative integer i such that $\sigma^i(x) \in K(z)_\sigma$ for all $x \in L$.

[6] We essentially reproduce the argument for the convenience of the reader.

Lemma 3.5. *(Cf. [1, Lemma 2.2].) Let A, A^*, H, A^H, i, π as above. Let A' be a difference subring of (A^H, σ^H) which is finitely generated over (A, σ). Then A' lifts to a difference subring of A^*, i.e. there exists a difference morphism $\psi : A' \to A^*$ such that $\psi|_A = i$ and $\pi\psi = Id_{A'}$.*

Proof. Say $A' = A[\boldsymbol{a}]_\sigma$, $\boldsymbol{a} = (a_1, \ldots, a_\ell)$, $a_i \in A^H$. By [1, Lemma 2.3], $Frac(A^H)/Frac(A)$ is a separable extension. Then so is $Frac(A')/Frac(A)$, $Frac(A') = Frac(A)(\boldsymbol{a})_\sigma$. By [7, Lemma (2.1)], there exists a transformal transcendence basis $\boldsymbol{b} \subset \boldsymbol{a}$ of $Frac(A')/Frac(A)$ s.t. $Frac(A)(\boldsymbol{a})_\sigma/Frac(A)(\boldsymbol{b})_\sigma$ is a separable extension. Any lifting of $\boldsymbol{b}$ readily yields a lifting of $A[\boldsymbol{b}]_\sigma$.

We now momentarily suppose that we are in characteristic 0 or that $Frac(A)$ is completely aperiodic. Suppose A_0 is any difference subring of A^H containing A and ψ_0 a lifting of A_0 in A^* satisfying the above conditions. By Theorem 3.4 it suffices for us to show that if $a \in A^H$ is transformally algebraic over A_0 and $Frac(A_0)(a)_\sigma/Frac(A_0)$ is separable, then ψ_0 extends to a lifting of $A_0[a]_\sigma$. Let a be such and $n \geqslant 0$ the least integer such that $A_0[Y]_\sigma$ contains a non-zero difference polynomial of order n with solution a. By [8, Chapter 5, §.14, Theorem X], the transcendence degree of $Frac(A_0)(a)_\sigma/Frac(A_0)$ is n. We can then select from $a, \sigma(a), \ldots, \sigma^n(a)$ a separating transcendence basis of

$$Frac(A_0)\big(a, \sigma(a), \ldots, \sigma^n(a)\big)/Frac(A_0)$$

say,

$$\boldsymbol{a_i} = \big(a, \sigma(a), \ldots, \sigma^{i-1}(a), \sigma^{i+1}(a), \ldots, \sigma^n(a)\big).$$

Let F be a minimal irreducible polynomial of $\sigma^i(a)$ over $A_0[\boldsymbol{a_i}]$, which can be viewed as $F(a, \sigma(a), \ldots, \sigma^{i-1}(a), X, \sigma^{i+1}(a), \ldots, \sigma^n(a))$ for some $F \in A_0[X_0, \ldots, X_n]$. Consider the associated difference polynomial $G(X) = F(X, \ldots, \sigma^n(X))$. Then $G(a) = 0$ and

$$\frac{\partial F}{\partial X_i}\big(a, \sigma(a), \ldots, \sigma^n(a)\big) \neq 0.$$

Let $\tilde{G} = G^{\psi_0}$, i.e. $\tilde{G}$ is obtained from G by making ψ_0 operate on the coefficients, and let $y \in A^*$ be such that $\pi(y) = a$. We now revert to the notation of Lemma 2.2 by putting $f = \tilde{G}$, in order to find a lifting of a which is a root of $\tilde{G}$. We have $v^*(f(y)) \notin H$ and $v^*(\frac{\partial f}{\partial X_i}(y, \sigma(y), \ldots, \sigma^n(y))) \in H$. Let $c \in A^*$ be such that $v^*(c) = \min_j v^*(\frac{\partial f}{\partial X_j}(y, \sigma(y), \ldots, \sigma^n(y)))$, so $v^*(c) \leqslant v^*(\frac{\partial f}{\partial X_i}(y, \sigma(y), \ldots, \sigma^n(y)))$. Since H is convex, $v^*(c) \in H$ and $c^{-2} f(y) \in A^*$ is a non-unit. Let W be a new indeterminate and put $\epsilon = cW$. Then

$$\begin{aligned} f(y+\epsilon) &= f(y) + \sum_{j=0}^{n} \frac{\partial f}{\partial X_j}\big(y, \sigma(y), \ldots, \sigma^n(y)\big) \cdot \sigma^j(c) \cdot \sigma^j(W) + c^2 R'(y, W) \\ &= c^2 \left(c^{-2} f(y) + \sum_{j=0}^{n} c'_j \sigma^j(W) + R'(y, W) \right) \end{aligned}$$

where $c'_j \in A^*$ at least one c'_j is a unit, and $R'(y, W) \in A^*[W]_\sigma$ and each of its monomials is of total degree at least 2. Evaluating at $W = 0$, the σ-henselianity of A^* gives that there exists $w \in A^*$ such that $c^{-2} f(y) + \sum_{j=0}^{n} c'_j \sigma^i(w) + R'(y, w) = 0$ and $w \in c^{-2} f(y) A^*$. Then $\alpha = y + cw$ is such that $\tilde{G}(\alpha) = 0$ and $\pi(\alpha) = a$. By sending $\sigma^i(a)$ to $\sigma^i(\alpha)$, $0 \leqslant i \leqslant n$, we readily extend ψ_0 to $A_0[a, \sigma(a), \ldots, \sigma^n(a)]$. Now in fact,[7] π is a difference ring homomorphism which sends $\psi_0(A_0)[\alpha]_\sigma$ onto $A_0[a]_\sigma$, and both these rings are domains and have transcendence degree n over $\psi_0(A_0)$ and A_0

[7] Thanks to the referee.

respectively. Hence the restriction of π to $\psi_0(A_0)[\alpha]_\sigma$ is injective, and an isomorphism, and yields our lifting.

We are left with the case where $Frac(A)$ is of characteristic $p > 0$ and not completely aperiodic. In this case[7] there are some integers $n > 1$ and m such that all the elements of A satisfy $\sigma^n(x) = x^{p^m}$, and so all the elements of A^* too. If $m \neq 0$, this implies that every difference subfield of $Frac(A^*)$ is perfect, so A' can be obtained from A by a tower of simple separable difference extensions and we can proceed as in the previous case. If $m = 0$ and $n = 1$, then we are reduced to the classical situation of Becker et al. [1, Lemma 2.2] and we are done. If $m = 0$ and $n > 1$, we have $\sigma^n(x) = x$ for all $x \in A$. Let $B_A = \{x \in A\colon\ \sigma(x) = x\}$, then for any $x \in A$ the polynomial $\prod_{j=0}^{n-1}(X - \sigma^j(x))$ belongs to $B_A[X]$ and so every element of A is integral over B_A of degree at most n, and the same holds for A^*, A^H and A'. This implies that we can express A' as $A[b'_1, \ldots, b'_k, a_1, \ldots, \sigma^{n-1}(a_1), \ldots, a_\ell, \ldots, \sigma^{n-1}(a_\ell)]$ where $\sigma^H(b'_i) = b'_i$, for all i and each a_j is integral of degree at most n over $A[b'_1, \ldots, b'_k]$. Appealing again to Becker et al., there is a ring homomorphism $\psi : A' \to A^*$ s.t. $\psi|_A = i$ and $\pi\psi = Id_{A'}$, and we can argue with π as before. □

End of proof of Theorem 3.1. Recall U, our non-principal ultrafilter on $\mathbb{N}$, and its functor $(\ )^*$.

Suppose the theorem is false. Then for each $N \in \mathbb{N}$, there exist $\alpha \in \mathbb{N}$ and $\boldsymbol{x} \in A$ such that $\alpha \neq 0$, $v(\boldsymbol{f}(\boldsymbol{x})) \geqslant N\alpha$, $\neg\exists \boldsymbol{y} \in A(\boldsymbol{f}(\boldsymbol{y}) = 0$ and $v(\boldsymbol{y} - \boldsymbol{x}) \geqslant \alpha)$. This gives sequences $\alpha_N \in \mathbb{N}$, $\boldsymbol{x}_N \in A$, for $N = 0, 1, \ldots$ which determine elements $\alpha \in \mathbb{N}^*$, $\boldsymbol{x} \in A^*$ satisfying $\alpha \neq 0$ and

$$v^*\big(\boldsymbol{f}(\boldsymbol{x})\big) \geqslant m\alpha, \quad \text{all } m \in \mathbb{N}, \tag{1}$$

$$\neg\exists \boldsymbol{y} \in A^* \quad \big(\boldsymbol{f}(\boldsymbol{y}) = 0 \text{ and } v^*(\boldsymbol{y} - \boldsymbol{x}) \geqslant \alpha\ \big). \tag{2}$$

Let $H = \{\beta \in \mathbb{Z}^*\colon\ -m\alpha \leqslant \beta \leqslant m\alpha,\ \text{for some } m \in \mathbb{N}\}$. Then H is a convex subgroup of $\mathbb{Z}^*$ containing $\mathbb{Z}$. Let $\pi : A^* \to A^H$ as above. From (1) it follows that $\boldsymbol{f}(\pi(\boldsymbol{x})) = \pi(\boldsymbol{f}(\boldsymbol{x})) = 0$. Let $A' = A[\pi(\boldsymbol{x})]_\sigma \subset A^H$. By Lemma 3.5 there is a lifting $\psi : A' \to A^*$. Let $\boldsymbol{y} = \psi(\pi(\boldsymbol{x}))$. Then $\boldsymbol{f}(\boldsymbol{y}) = 0$ and $\pi(\boldsymbol{y}) = \boldsymbol{x}$, so that $v^*(\boldsymbol{y} - \boldsymbol{x}) > \alpha$. But this contradicts (2), and we are done. □

Remarks.

(1) Our main results also apply to certain operators derived from automorphisms. E.g. in Witt vectors one has the delta-ring operator [17]

$$\delta(x) = \big(\sigma_p(x) - x^p\big)/p$$

(or p-derivation, see [6]). So one has $\sigma_p(x) = x^p + p\delta(x)$. From these relations one computes polynomial relations connecting the iterates σ_p^n and δ^n. In particular there are polynomials $P_n(X_0, \ldots, X_n) \in \mathbb{Z}[X_0, \ldots, X_n]$ and integers $k_n \geqslant 1$, such that

$$\delta^n(x) = \frac{1}{p^n}\sigma_p^n(x) + \frac{1}{p^{k_n}}P_n\big(x, \sigma_p(x), \ldots, \sigma_p^{n-1}(x)\big).$$

For example,

$$\delta^2(x) = \frac{1}{p^2}\sigma_p^2(x) + \frac{1}{p^{p+1}}\big(-p^{p-1}\sigma_p(x)^p - \big(\sigma_p(x) - x^p\big)^p\big).$$

Let $A = W[\widetilde{\mathbb{F}}_p]$ and $A[\boldsymbol{X}]_\delta$ be the analog of $A[\boldsymbol{X}]_\sigma$ but with δ playing the role of σ. Using the above identities to make substitutions and then clear denominators, one can deduce the analog of Theorem 3.1 and Corollary 3.2, e.g. suppose $g_i \in A[\boldsymbol{X}]_\delta$, $i = 1, \ldots, m$, are such that for all integer $N \geqslant 1$, there exists $\boldsymbol{x} \in A$ such that $g_i(\boldsymbol{x}) \equiv 0 \bmod p^N$, $i = 1, \ldots m$, then there exists $\boldsymbol{y} \in A$ such that $g_i(\boldsymbol{y}) = 0$, $i = 1, \ldots m$.

(2) The same methods yield an analog of [13] (cf. [9, Theorem (A.4)]). Namely, let (A,σ) be a difference ring which is also a domain of characteristic 0, let $f_1,\dots,f_m \in A[\boldsymbol{X}]_\sigma$ and $\boldsymbol{f}=(f_1,\dots,f_m)$. Then there exist an integer $c(\boldsymbol{f})\geqslant 1$ and a non-zero element $a(\boldsymbol{f})\in A$ with the following property: for each σ-henselian valuation ring $V\supset A$ which is also a difference ring extension of A, with associated valuation v satisfying $v(\sigma(x))=v(x)$, and value group Γ, for each $g\in\Gamma$, $g>0$, and for each $\boldsymbol{x}\in V$ such that $v(\boldsymbol{f}(\boldsymbol{x}))>c(\boldsymbol{f})\,.\,g+v(a(\boldsymbol{f}))$, there exists $\boldsymbol{y}\in V$ such that $\boldsymbol{f}(\boldsymbol{y})=0$ and $v(\boldsymbol{y}-\boldsymbol{x})>g$.

(3) In the case of $(W[\widetilde{\mathbb{F}}_p],\sigma_p)$, there is a somewhat more direct argument to get Corollary 3.2. It is close to [23, §.3] and "avoids" Lemma 3.5, using the universal property of Witt vectors and the model-completeness[8] of the first-order theory of $(W[\widetilde{\mathbb{F}}_p],\sigma_p)$ [2,26,5]. We gave the details in [4, théorème 2.1].

4. Derivations

Valued differential fields where the valuation and the derivative have a close interaction were studied by Scanlon [24]. In fact, he gives a common setup covering at the same time difference and differential valued fields. We did not do this here as the differential characteristic p case needs a somewhat different treatment. We will formulate the basic notions in terms of rings.

Definition 4.1. (Cf. [24].) Let (A,D) be a differential ring which is a valuation ring. We say that (A,D) is a D-valuation ring if a divides Da, for all $a\in A$.

In particular in a D-valuation ring (A,D), the maximal ideal is closed under D and D induces a derivation on the residue field. Again, natural examples are given by power series rings $k[[T]]$ over a differential field (k,δ) with $D(\sum a_nT^n)=\sum\delta(a_n)T^n$ (see [24] for further examples with power series).

A D-valuation ring will be said to be excellent if its underlying ring is. Again, [24] gives the appropriate notion of *D-henselian*,[9] and natural examples are given by the power series above when the base differential field (k,δ) is such that linear differential equations have enough solutions to provide a basic Newton approximation process.

Definition 4.2. *Let (A,D) be a D-valuation ring. We say (A,D) is* D-henselian*, if for all $f\in A\{X\}$, given by $f(X_0,X_1,\dots,X_n)\in A[X_0,\dots,X_n]$, i.e. $f(X)=f(X,DX,\dots,D^nX)$, and for all $y\in A$ such that $f(y)$ is a non-unit but $\frac{\partial f}{\partial X_i}(y,Dy,\dots,D^ny)$ is a unit for at least one i, then there exists $x\in A$ such that $f(x)=0$ and $x-y\in f(y)A$.*

The main results are, mutatis mutandis, the same as in Section 3 and follow formally in the same way from a key lifting property analog to Lemma 3.5.

Theorem 4.3. *Let (A,D) be a D-valuation ring which is a D-henselian excellent discrete valuation ring. In characteristic $p>0$ we further assume that the iterates D^i satisfy no polynomial identity. Let t be a uniformizing parameter of A, let $f_1,\dots,f_m\in A\{\boldsymbol{X}\}$, and $\boldsymbol{f}=(f_1,\dots,f_m)$. Then there exists an integer $N\in\mathbb{N}$, depending on $\boldsymbol{f}$, such that for all $\alpha\in\mathbb{N}$, $\alpha>0$, and for all $\boldsymbol{x}\in A$ such that $\boldsymbol{f}(\boldsymbol{x})\equiv 0 \bmod t^{\alpha N}$, there exists $\boldsymbol{y}\in A$ such that $\boldsymbol{f}(\boldsymbol{y})=0$ and $\boldsymbol{y}\equiv\boldsymbol{x}\bmod t^\alpha$.*

We will only prove the appropriate lifting lemma, the only significant change in the proof being in the positive characteristic case where we will need the extra assumption that the derivation satisfies *no identity*.

The setting is a D-valuation ring (A,D) which is a D-henselian excellent discrete valuation ring, t is a uniformizing parameter, v the valuation associated to A and $k=A/(t)$ the residue field.

[8] See Section 5 below.

[9] Similar schemes were considered in [11] for differential operators.

Lemma 4.4. *With the same notation as in Lemma* 3.5 *with U and* $(\,)^*$ *etc., let* D^H *be the induced derivation on* A^H *via the natural projection* π, *and let* A' *be a differential subring of* (A^H, D^H) *which is finitely generated over* (A, D). *Then* A' *lifts to a differential subring of* A^*, *i.e. there exists a differential morphism* $\psi : A' \to A^*$ *such that* $\psi|_A = i$ *and* $\pi\psi = 1_{A'}$.

Proof. Let $A' = A\{\boldsymbol{a}\}$, $\boldsymbol{a} = (a_1, \ldots, a_n)$, $a_i \in A^H$. Again, by [1, Lemma 2.3], $Frac(A')/Frac(A)$ is a separable extension, $Frac(A') = Frac(A)\langle\boldsymbol{a}\rangle$.

By [18, Chapter II, §.9—§.10, Theorems 4 and 5], there exists a differential transcendence basis $\boldsymbol{b} \subseteq \boldsymbol{a}$ s.t. $\boldsymbol{b}$ is differentially algebraically independent, $Frac(A)\langle\boldsymbol{a}\rangle/Frac(A)\langle\boldsymbol{b}\rangle$ is a separable extension, and every element of $Frac(A)\langle\boldsymbol{a}\rangle$ is differentially separable over $Frac(A)\langle\boldsymbol{b}\rangle$. Any lifting of $\boldsymbol{b}$ readily yields a lifting of $A\{\boldsymbol{b}\}$. Let $A_0 = A\{\boldsymbol{b}\}$ and ψ_0 a lifting of A_0 as above. By [18, Chapter II, §.8, Proposition 9], and the extra assumption of no identity in characteristic p, we can assume that $Frac(A)\langle\boldsymbol{a}\rangle = Frac(A_0)\langle a\rangle$ for a single element $a \in A\{\boldsymbol{a}\}$.

Then, by [18, Chapter II, §.11, Corollary 1], the extension $Frac(A_0)\langle a\rangle/Frac(A_0)$ is in fact finitely generated as a field extension, in particular it has finite transcendence degree, say r. By [27, Theorem 7], $a, Da, \ldots, D^{r-1}a$ are algebraically independent over $Frac(A_0)$, $D^r a$ is separable over $Frac(A_0)(a, Da, \ldots, D^{r-1}a)$, and $Frac(A_0)\langle a\rangle = Frac(A_0)(a, Da, \ldots, D^r a)$.

Let F be a minimal irreducible polynomial of $D^r a$ over $A_0[a, Da, \ldots, D^{r-1}a]$, which can be viewed as $F(a, Da, \ldots, D^{r-1}a, X)$ for some $F \in A_0[X_0, \ldots, X_r]$. Consider the associated differential polynomial $G(X) = F(X, \ldots, D^r X)$. Then $G(a) = 0$ and

$$\frac{\partial F}{\partial X_r}\big(a, Da, \ldots, D^r a\big) \neq 0.$$

Let $\tilde{G} = G^{\psi_0}$, i.e. $\tilde{G}$ is obtained from G by making ψ_0 operate on the coefficients, and let $y \in A^*$ be such that $\pi(y) = a$. We put $f = \tilde{G}$ and do a calculation similar to the difference case. Again $v^*(f(y)) \notin H$ and $v^*(\frac{\partial f}{\partial X_r}(y, Dy, \ldots, D^r y)) \in H$. Let $c_j = \frac{\partial f}{\partial X_j}(y, Dy, \ldots, D^r y)$, $0 \leqslant j \leqslant r$, so $v^*(c_r) \in H$. Recall that in A^*, x always divides Dx. Let W be a new indeterminate and put $\epsilon = c_r W$. Then

$$f(y + \epsilon) = f(y) + \sum_{j=0}^{r} c_j D^j(c_r W) + S(y, c_r W)$$

where $S(y, Z) \in A^*\{Z\}$ and each of its monomial (in $Z, DZ, \ldots$) is of total degree at least 2. Using Leibniz' rule, for each j, $D^j(c_r W)$ can be written as a polynomial in the $D^i W$, $0 \leqslant i \leqslant j$, and the coefficient of $D^j W$ is c_r. Thus, when writing $\sum_{j=0}^{r} c_j D^j(c_r W)$ as a polynomial in $W, DW, \ldots, D^r W$, the coefficient of $D^r W$ is c_r^2 and $v^*(c_r^2) \in H$. Let $c \in A^*$ be a coefficient of some $D^j W$ occurring in this expression with minimum value. Then $v^*(c) \in H$, and c divides c_r^2; hence c divides all coefficients of $S(y, c_r W)$ when expressed as a polynomial in $W, DW, \ldots D^r W$. This gives

$$f(y + \epsilon) = c\left(c^{-1} f(y) + \sum_{j=0}^{r} c'_j D^j W + R(y, W)\right)$$

where $R(y, W) \in A^*\{W\}$, all monomials in $R(y, W)$ have total degree at least 2, and the c'_j are in A^*, with at least one c'_j a unit. As in the difference case, the D-henselianity of A^* gives some $w \in A^*$ such that $f(y + c_r w) = 0$. Then $\alpha = y + c_r w$ is such that $\tilde{G}(\alpha) = 0$ and $\pi(\alpha) = a$. By sending $D^i a$ to $D^i \alpha$, $0 \leqslant i \leqslant r$, we readily extend ψ_0 to the ring $A_0[a, Da, \ldots, D^r a]$, and moreover this is also a differential ring lifting as the differential structure extending that of A_0 is uniquely determined by $D(D^i a) = D^{i+1} a$, or one can argue with π as in the difference case. □

5. Nullstellensatz

In his beautiful paper [19], Kochen gives a p-adic analog of Hilbert's 17th problem by characterizing the rational functions over the p-adic numbers $\mathbb{Q}_p$ which take only integral values: they are exactly those which satisfy a relation[10] of the form $f^n + \sum_{i=0}^{n-1} a_i f^i = 0$, where $a_i = \frac{s_i}{1+pt_i}$, $s_i, t_i \in \mathbb{Z}[\gamma(\mathbb{Q}_p(x_1, \ldots, x_m))]$, $\gamma(x) = \frac{1}{p}\frac{x-x^p}{(x-x^p)^2-1}$. The function $\gamma(x)$ takes only integral values and replaces the square function $x \mapsto x^2$ in Artin's proof. Using this result, Kochen goes on to prove a p-adic Nullstellensatz via the approximation property in the p-adic integers. We have checked elsewhere [3] for the field of Witt vectors $W(\widetilde{\mathbb{F}}_p) = Frac(W[\widetilde{\mathbb{F}}_p])$ a difference field analog for difference rational functions taking integral values. We can then similarly deduce a Nullstellensatz for difference equations (Theorem 5.5).

We will gather the key facts from [3]. The main auxiliary result is the model-completeness of the first-order theory of the Witt vectors $W(\widetilde{\mathbb{F}}_p)$ with their Frobenius automorphism [2,26,5]. We roughly recall A. Robinson's basic concept of *model-completeness* (see [20]). A substructure $\mathcal{M}$ of a structure $\mathcal{N}$ is said to be an *elementary substructure*, if for each sentence φ of first-order logic formulated in terms of the basic operations and relations of $\mathcal{M}$ and $\mathcal{N}$ *and parameters from* $\mathcal{M}$, we have that φ holds in $\mathcal{N}$ iff φ holds in $\mathcal{M}$. In particular, any system of equations and inequations with parameters in $\mathcal{M}$ which has a solution in $\mathcal{N}$ already has a solution in $\mathcal{M}$. An example is given by an extension of algebraically closed fields $\mathcal{M} \subseteq \mathcal{N}$. A first-order theory is said to be *model-complete*, if whenever one of its model $\mathcal{M}$ is a substructure of another model $\mathcal{N}$, then it is an elementary substructure. An example is given by the first-order theory of algebraically closed fields.

In the discussion below p will be a fixed prime, and v_p will denote the p-adic valuation on $W(\widetilde{\mathbb{F}}_p)$. In a difference field (K, σ) we consider the multiplicative group $G_{\sigma,K} = \{\sigma(x)x^{-1}\colon\ x \in K^\times\}$ and the function $\gamma_\sigma(x) = \frac{1}{p}\frac{\sigma(x)-x^p}{(\sigma(x)-x^p)^2-1}$. For a field K, $K(\mathbf{X})_\sigma$ stands for the field of fractions of $K[\mathbf{X}]_\sigma$. A difference valuation ring (A, σ) will be called *wittian*, if it has characteristic zero, $\max(A) = pA$, and for all $x \in A$ we have $(\sigma(x) - x^p) \in \max(A)$ and x, $\sigma(x)$ divide each other. A valued difference field (K, v, σ) will be called wittian if it is the field of fractions of a wittian difference valuation ring and v is the corresponding valuation. For a valued field (K, v) we will denote by V_K its valuation ring. Let (K, v, σ) be wittian and (L, σ) an extension field of (K, σ). We will denote by $W_{L/K}$ the set of valuation rings of L above V_K which make L wittian.

Proposition 5.1. *(See [3].)*

(1) *[19, Lemma 3] Let (K, v) be a valued field, L an extension field of K, and A a subring of L s.t. $V_K = A \cap K$. Let $T = \{1 + ma\colon\ m \in \max(V_K),\ a \in A\}$. Then the integral closure of the ring of fractions $A[T^{-1}]$ is the intersection of all valuation rings V_L of L such that $A \subseteq V_L$ and $V_K = V_L \cap K$.*

(2) *Let (A, σ) be a difference valuation ring of characteristic 0 s.t. $p \in \max(A)$ and $x, \sigma(x)$ divide each other for all $x \in A$. Then (A, σ) is wittian if and only if $v(\gamma_\sigma(Frac(A))) \geqslant 0$.*

(3) *[5] Any wittian (K, σ) embeds in a model of the first-order theory of $(W(\widetilde{\mathbb{F}}_p), v_p, \sigma_p)$.*

(4) *Suppose (K, v, σ) wittian and (L, σ) an extension of (K, σ). Then $W_{L/K} \neq \emptyset$ if and only if $\frac{1}{p} \notin V_K[\gamma_\sigma(L), G_{\sigma,L}]$.*

(5) *Let $(K, v, \sigma) = (W(\widetilde{\mathbb{F}}_p), v_p, \sigma_p)$, and (L, σ) an extension of (K, σ) s.t. $W_{L/K} \neq \emptyset$. Consider $A = \mathbb{Z}[\gamma_\sigma(L), G_{\sigma,L}]$ and $y \in L$. Then $y \in \bigcap_{V \in W_{L/K}} V$ if and only if y is integral over the ring of fractions $A[(1 + pA)^{-1}]$.*

(6) *Let $(K, v, \sigma) = (W(\widetilde{\mathbb{F}}_p), v_p, \sigma_p)$, and $r \in K(\boldsymbol{X})_\sigma$, and $A = \mathbb{Z}[\boldsymbol{X}, \gamma_\sigma(K(\boldsymbol{X})_\sigma), G_{\sigma,K(\boldsymbol{X})_\sigma}]$. Then $v(r(\boldsymbol{x})) \geqslant 0$ for all $\boldsymbol{x} \in V_K$ where r is defined, if and only if r is integral over the ring of fractions $A[(1 + pA)^{-1}]$.*

[10] For the even more telling analogy with $n = 1$, see [22, Theorem 7.7].

Definition 5.2. (Cf. [19].) Let (K,σ,v) be a valued difference field and $r \in K(\mathbf{X})_\sigma$. We say that r is *regular on* V_K if there is $\lambda \in K^\times$ such that $v(r(\mathbf{x})) \geqslant v(\lambda)$, for all $\mathbf{x} \in V_K$ where $r(\mathbf{x})$ is defined.

Proposition 5.3. *Let* $(K,\sigma,v) = (W(\widetilde{\mathbb{F}}_p),\sigma_p,v_p)$, *and* $r \in K(\mathbf{X})_\sigma$. *Set* $A = \mathbb{Z}[\mathbf{X},\gamma_\sigma(K(\mathbf{X})_\sigma),G_{\sigma,K(\mathbf{X})_\sigma}]$ *and consider the ring of fractions* $R = A[(1+pA)^{-1}]$. *Then* r *is regular on* V_K *if and only if* r *is integral over* $R\cdot K$.

Proof. By Proposition 5.1(6), $v(\lambda^{-1}r(\mathbf{x})) \geqslant 0$ for all $\mathbf{x} \in V_K$ s.t. $r(\mathbf{x})$ is defined, if and only if $\lambda^{-1}r$ is integral over R, whence the result. □

The following lemma follows directly from Corollary 3.2.

Lemma 5.4. *Let* $(K,\sigma,v) = (W(\widetilde{\mathbb{F}}_p),\sigma_p,v_p)$ *and* $h \in K[\mathbf{X}]_\sigma$. *Then* h *has no zero in* V_K *if and only if* h^{-1} *is regular on* V_K.

We then argue as in [19, Lemma 5] to deduce the Nullstellensatz. Note that $R\cdot K = R\cdot K[\mathbf{X}]_\sigma$.

Theorem 5.5 *(Nullstellensatz). Let* K *and* R *be as in the proposition above and* $f_1,\dots,f_m \in K[\mathbf{X}]_\sigma$. *If* $f_1,\dots,f_m$ *have no common zero on* V_K, *then* $(f_1,\dots,f_m)_{R\cdot K} = R\cdot K$, *where* $(f_1,\dots,f_m)_{R\cdot K}$ *denotes the ideal generated by the* f_i *in the ring* $R\cdot K$.

Proof. Let $f = \sum_{i=1}^m p^{i-1}f_i^m$, then $f(\mathbf{x}) = 0$ iff $f_1(\mathbf{x}) = 0,\dots,f_m(\mathbf{x}) = 0$. Hence f has no zero in V_K and f^{-1} is integral over $R\cdot K$. Since $f \in R\cdot K$, then f^{-1} must be in $R\cdot K$, and we are done. □

Note that this Nullstellensatz can be proved by developing a suitable ideal theory, e.g. in the style of [29].

Also, the results above hold for (K,v,σ) *elementarily equivalent* to $(W(\widetilde{\mathbb{F}}_p),v_p,\sigma_p)$, i.e. model of the first-order theory of $(W(\widetilde{\mathbb{F}}_p),v_p,\sigma_p)$.

D. Haskell has pointed out to us that Kochen's lemma (Proposition 5.1(1)) can also be applied to differential valuation rings to get a similar characterization of differential rational functions taking only integral values (see [15]). One then can apply the appropriate approximation theorem to get a differential Nullstellensatz as above. We leave the details to the reader.

References

[1] J. Becker, J. Denef, L. Lipshitz, L. van den Dries, Ultraproducts and approximation in local rings I, Invent. Math. 51 (1979) 189–203.
[2] L. Bélair, A. Macintyre, L'automorphisme de Frobenius des vecteurs de Witt, C. R. Acad. Sci. Paris Sér. I 331 (2000) 1–4.
[3] L. Bélair, Fonctions rationnelles aux différences à valeurs entières dans les vecteurs de Witt, C. R. Acad. Sci. Paris Sér. I 339 (2004) 83–86.
[4] L. Bélair, Équations aux différences dans les vecteurs de Witt, C. R. Acad. Sci. Paris Sér. I 340 (2005) 99–102.
[5] L. Bélair, A. Macintyre, T. Scanlon, Model theory of the Frobenius on the Witt vectors, Amer. J. Math. 129 (2007) 665–721.
[6] A. Buium, An approximation property for Teichmüller points, Math. Res. Lett. 3 (1996) 453–457.
[7] Z. Chatzidakis, Generic automorphisms of separably closed fields, Illinois J. Math. 45 (2001) 693–733.
[8] R.M. Cohn, Difference Algebra, Wiley, 1965.
[9] L. van den Dries, Model theory of fields, decidability, and bounds for polynomial ideals, Doctoral thesis, Rijkuniversiteit te Utrecht, Netherlands, 1978.
[10] A. Duval, Lemmes de Hensel et factorisation formelle pour les opérateurs aux différences, Funkcial. Ekvac. 26 (1983) 349–368.
[11] B. Dwork, P. Robba, On ordinary linear p-adic differential equations, Trans. Amer. Math. Soc. 231 (1977) 1–46.
[12] M. Greenberg, Rational points in henselian discrete valuation rings, Publ. Math. Inst. Hautes Études Sci. 31 (1966) 59–64.
[13] M. Greenberg, Strictly local solutions of diophantine equations, Pacific J. Math. 51 (1974) 143–153.
[14] N. Guzy, Quelques remarques sur les corps D-valués, C. R. Acad. Sci. Paris Sér. I 343 (2006) 689–694.
[15] D. Haskell, Y. Yaffe, Ganzestellensätze in theories of valued fields, preprint.
[16] N. Jacobson, Basic Algebra II, Freeman, 1987.
[17] A. Joyal, δ-anneaux et vecteurs de Witt, C.R. Math. - Math. Rep. Acad. Sci. Canada 7 (1985) 177–182.
[18] E.R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, 1973.

[19] S. Kochen, Integral valued rational functions over p-adic numbers: A p-adic analogue of the theory of real fields, in: W.J. LeVeque, E.G. Strauss (Eds.), Proc. Sympos. Pure Math., vol. XII, Amer. Math. Soc., 1969, pp. 57–73.
[20] D. Marker, Model Theory: An Introduction, Springer, 2002.
[21] D. Popescu, Artin approximation, in: M. Hazewinkel (Ed.), Handbook of Algebra, vol. 2, Elsevier, 2003, pp. 321–356.
[22] A. Prestel, P. Roquette, Formally p-Adic Fields, Springer, 1984.
[23] A. Robinson, Elementary embeddings of fields of power series, J. Number Theory 2 (1970) 237–247.
[24] T. Scanlon, A model-complete theory of valued D-fields, J. Symbolic Logic 65 (2000) 1758–1784.
[25] T. Scanlon, Diophantine geometry from model theory, Bull. Symbolic Logic 7 (2001) 37–57.
[26] T. Scanlon, Quantifier elimination for the relative Frobenius, in: F.V. Kuhlmann, et al. (Eds.), Valuation Theory and Its Applications, vol. II, Saskatoon, SK, 1999, Amer. Math. Soc., 2003, pp. 323–352.
[27] A. Seidenberg, Some basic theorems in differential algebra (characteristic p, arbitrary), Trans. Amer. Math. Soc. 73 (1952) 174–190.
[28] J.-P. Serre, Local Fields, Springer, 1979.
[29] A. Srhir, P-adic ideals of p-rank d and the p-adic Nullstellensatz, J. Pure Appl. Algebra 180 (2003) 299–311.